UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,133	08/10/2001	Russell Andrew Fink	00-4045	6468

32127 7590 10/19/2006

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD, SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/928,133	FINK ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to Applicant's Remarks and Amendments filed July 27, 2006.

Claims 1 and 4 are amended.

Claims 1-24 are herein considered.

Response to Arguments

Applicant's arguments with respect to the Examiner's incorporation of PCT Patent Application Publication No. WO 97/26734 within Kraemer et al. (U.S. Patent No. 5,798,706) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of PCT Patent Application Publication No. WO97/26734.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kraemer et al. (U.S. Patent No. 5,798,706), and further in view of International Patent Application Publication No. WO 97/26734.

As per **Claim 1**, Kraemer et al. discloses an apparatus for detecting adversarial activity on a network, comprising a memory adapted to store a host table (see col.3 lines 46-60); a key exchanger; a translator adapted to translate predetermined portions of packet header information of a data packet, wherein the predetermined portions include an address (see col.4 lines 33-46); a mapping device adapted to map the address to the host table (see col.3 line 60 thru col.4 line 2); a host resolution device adapted to issue a request to the network to resolve the address when the address does not match an entry in the host table and to supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and an actuator adapted to trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

Kraemer fails to specifically mention a key exchanger adapted to derive a cipher key and a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key.

WO 97/26734 teaches a key exchanger adapted to derive a cipher key (page 2) and a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (page 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the Kraemer system a key exchanger adapted to derive a cipher key and a translator adapted to translate predetermined portions of

packet header information of a data packet according to a cipher algorithm keyed by the cipher key as described in WO 97/26734 to provide enhanced security capabilities.

As per **Claim 2**, the combination of Kraemer and WO 97/26734 discloses an apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 3**, the combination of Kraemer and WO 97/26734 discloses an apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered (see Kraemer col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim** 4, the combination of Kraemer and WO 97/26734 discloses an apparatus as set forth in Claim 1, further comprising a host resolution device adapted to derive the host table using an address resolution protocol (see Kraemer col.4 lines 48-52).

As per **Claim 5**, the combination of Kraemer and WO 97/26734 discloses an apparatus as set forth in Claim 1, further comprising a network device adapted to place the data packet onto a network when the address maps to the host table (Kraemer col.1 line 66 through col.2 line 9 and col.2 lines 27-31).

As per **Claim 6**, Kraemer et al. discloses a method for detecting adversarial activity on network, comprising storing a host table (see col.3 lines 46-60); deriving a key; translating predetermined portions of packet header information of a data packet, wherein the predetermined portions include an address (see col.4 lines 33-46); mapping the address the host table (see col.3 line 60 thru col.4 line 2); issuing a request to the

network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

Kraemer fails to specifically mention a key exchanger adapted to derive a cipher key and a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key.

WO 97/26734 teaches a key exchanger adapted to derive a cipher key (page 2) and a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (page 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the Kraemer system a key exchanger adapted to derive a cipher key and a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key as described in WO 97/26734 to provide enhanced security capabilities.

As per **Claim 7**, the combination of Kraemer and WO 97/26734 discloses a method as set forth in Claim 6, further comprising logging the data packet when the address does not match an entry in the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 8**, the combination of Kraemer and WO 97/26734 discloses a method as set forth in Claim 6, further comprising signaling an alarm when the security device is triggered (see Kraemer col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 9,** the combination of Kraemer and WO 97/26734 discloses a method as set forth in Claim 6, further comprising deriving the host table using an address resolution protocol (see Kraemer col.4 lines 48-52).

As per **Claim 10**, the combination of Kraemer and WO 97/26734 discloses a method as set forth in Claim 6, further comprising placing the data packet onto a network when the address maps to the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 11**, Kraemer et al. discloses a device for detecting adversarial activity on a network, comprising means for storing a host table (see col.3 lines 46-60); means for deriving a key; means for translating predetermined portions of header information of a data packet, wherein the predetermined portions include an address (see col.4 lines 33-46); means for mapping the address to the host table (see col.3 line 60 thru col.4 line 2); means for issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and means for triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

Kraemer fails to specifically mention means to derive a cipher key and means to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key.

WO 97/26734 teaches the means to derive a cipher key (page 2) and the means to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (page 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the Kraemer system the means to derive a cipher key and the means translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key as described in WO 97/26734 to provide enhanced security capabilities.

As per **Claim 12**, the combination of Kraemer and WO 97/26734 discloses a device as set forth in Claim 11, further comprising means for logging the data packet when the address does not match an entry in the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 13**, the combination of Kraemer and WO 97/26734 discloses a device as set forth in Claim 11, further comprising means for signaling an alarm when the security device is triggered (see Kraemer col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 14**, the combination of Kraemer and WO 97/26734 discloses a device as set forth in Claim 11, further comprising means for deriving the host table using an address resolution protocol (see Kraemer col.4 lines 48-52).

As per **Claim 15**, the combination of Kraemer and WO 97/26734 discloses a device as set forth in Claim 11, further comprising means for placing the data packet network when the address maps to the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 16**, Kramer et al. discloses a bastion host adapted for processing packet header information of a data packet, the bastion host being operable to store a host table (see col.3 lines 46-60) derive a key; translate predetermined portions of packet header information of a data packet, wherein the predetermined portions include an address (see col.4 lines 33-46); map the address to the host table (see col.3 line 60 thru col.4 line 2); issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

Kraemer fails to specifically mention deriving a cipher key and translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key.

WO 97/26734 teaches deriving a cipher key (page 2) and translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (page 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the Kraemer system the means to derive a cipher key and the means translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key as described in WO 97/26734 to provide enhanced security capabilities.

As per **Claim 17**, the combination of Kraemer and WO 97/26734 discloses the bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 18,** the combination of Kraemer and WO 97/26734 discloses the bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered (see Kraemer col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 19**, the combination of Kraemer and WO 97/26734 discloses the bastion host as set forth in Claim 16, the bastion host being further operable to derive the host table using an address resolution protocol (see Kraemer col.4 lines 48-52).

As per **Claim 20**, the combination of Kraemer and WO 97/26734 discloses the bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table (see Kraemer col.4 lines 3-5 and 26-31).

As per **Claim 21**, the combination of Kraemer and WO 97/26734 discloses the apparatus as set forth in Claim 1, wherein said key exchanger is further adapted to

repeatedly derive a cipher key with the cipher key derived by said key exchanger over time (see WO 97/26734 page 8 lines 10-15, and page 11 line 31 thru page 13 line 5).

As per **Claim 22**, the combination of Kraemer and WO 97/26734 discloses the method as set forth in Claim 6, wherein deriving the cipher key comprises repeatedly deriving a cipher key such that the resulting cipher key changes over time (see WO 97/26734 page 8 lines 10-15, and page 11 line 31 thru page 13 line 5).

As per **Claim 23**, the combination of Kraemer and WO 97/26734 discloses the device as set forth in Claim 11, wherein said means for deriving a cipher key is further adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time (see WO 97/26734 page 8 lines 10-15, and page 11 line 31 thru page 13 line 5).

As per **Claim 24**, the combination of Kraemer and WO 97/26734 discloses the bastion host as set forth in Claim 16, wherein said the bastion host is further operable to repeatedly derive a cipher key such that the resulting cipher key changes over time (see WO 97/26734 page 8 lines 10-15, and page 11 line 31 thru page 13 line 5).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. Teslovich

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER